Rilevamento e soluzione alternativa agli attacchi KRACK wireless lato client

Sommario

Introduzione

Il 16 ottobre, è stato reso pubblico un insieme di vulnerabilità ampiamente conosciute come KRACK che influenzano diversi protocolli usati nelle reti WiFi. Tali modifiche influiscono sui protocolli di sicurezza utilizzati sulle reti WPA/WPA2 e potrebbero compromettere la riservatezza o l'integrità dei dati trasmessi tramite una connessione wireless.

Il livello pratico di impatto varia in modo significativo in ogni scenario, inoltre non tutte le implementazioni lato client sono interessate nello stesso modo.
Gli attacchi usano diversi scenari intelligenti di "test negativi" in cui le transizioni di stato non correttamente definite sugli standard wireless vengono provate, e nella maggior parte dei casi, non gestite correttamente dal dispositivo interessato. Non è contro gli algoritmi di crittografia utilizzati per proteggere WPA2, ma su come vengono effettuate le negoziazioni di autenticazione e protocollo durante la protezione della connessione wireless.

La maggior parte degli scenari di vulnerabilità sono stati segnalati per i clienti, dove il possibile attacco tipico utilizzerà falsi Ap come "uomo nel mezzo" per intercettare e iniettare fotogrammi specifici durante le negoziazioni di sicurezza tra il cliente e l'AP reale (CVE-2017-13077, CVE-2017-13078, CVE-2017-13080, CVE-2017-13080, CVE-2033 81). Questi sono gli elementi principali del presente documento

Èstato descritto uno scenario che attacca l'infrastruttura AP che fornisce servizi di roaming veloce 802.11r (FT) (CVE-2017-1382), che è fissato sul codice AireOS recentemente rilasciato

Restano 4 attacchi contro protocolli specifici del client: STK, TDLS, WNM, che non sono direttamente supportati dall'infrastruttura AireOS (CVE-2017-13084 CVE-2017-13086 CVE-2017-13087 CVE-2017-13088) e non rientrano nell'ambito di applicazione del presente documento

In pratica, un utente malintenzionato potrebbe decifrare il traffico della sessione interessata o inserire i frame in una o due direzioni. Non consente di decodificare il traffico esistente prima dell'attacco, né fornisce un meccanismo per "ottenere" le chiavi di crittografia di tutti i dispositivi in un determinato SSID o le relative password PSK o 802.1x

Le vulnerabilità sono reali e hanno un impatto significativo, ma non significano che le reti protette da WPA2 siano "interessate per sempre", in quanto il problema può essere risolto migliorando le implementazioni sia sul lato client che su quello AP, per funzionare correttamente in quegli *scenari di test negativi* che attualmente non sono gestiti in modo affidabile

Cosa deve fare un cliente:

- Per le vulnerabilità del lato AP: Aggiorna è l'azione consigliata se si utilizza FT. se FT non è necessario per i servizi voce/video, valutare se la funzionalità FT deve essere disabilitata fino al completamento dell'aggiornamento al codice fisso. Se si utilizza la voce, valutare se CCKM è fattibile (il lato client deve supportare) o eseguire l'aggiornamento al codice fisso. Se non viene utilizzato alcun FT/802.11r, non è necessario aggiornare
- Per migliorare la visibilità delle vulnerabilità sul lato client: verificare che sia abilitato il rilevamento rogue, che copra tutti i canali, e che sia stata creata una regola per segnalare "managed SSID" come dannoso. Implementare inoltre le modifiche alle configurazioni dei tentativi EAPoL che possono limitare o bloccare completamente gli attacchi da eseguire, come descritto in questo documento

Il principale consulente di riferimento è disponibile all'indirizzo https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-20171016-wpa. T

Componenti usati

Nel documento si fa riferimento ai Wireless Controller con versione 8.0 o successive.

Requisiti

Èrichiesta la conoscenza del contenuto dell'avviso di sicurezza di cui sopra.

Per gli attacchi WPA KRACK, ci sono due azioni principali che possiamo intraprendere per proteggere i client che non sono ancora stati patch.

1. Protezione tentativi EAPoL (EAP over LAN)

2. Funzioni di rilevamento e rappresentazione del punto di accesso (AP) per rilevare se gli strumenti di attacco sono in uso

Protezione da attacchi EAPoL

Per le vulnerabilità da -2017-13077 a 81, è relativamente facile prevenire che i client siano interessati, utilizzando un contatore dei tentativi EAPoL impostato su zero. Questa configurazione è disponibile in tutte le versioni WLC

Perché funziona

L'attacco richiede almeno un ulteriore tentativo EAPoL generato dall'autenticatore durante l'handshake a 4 vie o durante la rotazione della chiave di trasmissione. Se si blocca la generazione di tentativi, l'attacco non può essere applicato alla chiave temporanea Pairwise (PTK)/alla chiave temporanea Groupwise (GTK).

Possibile impatto

1. client lenti o che potrebbero interrompere l'elaborazione iniziale di EAPoL M1 (ossia il primo messaggio dello scambio di chiavi a 4 vie). Questo si verifica su alcuni piccoli client o telefoni, che potrebbero ricevere il M1 e non essere pronti per elaborarlo dopo la fase di autenticazione dot1x, o farlo troppo lentamente per soddisfare un timer di ritrasmissione breve

2. Scenari con ambiente RF errato o connessioni WAN tra AP e WLC, che possono causare il rifiuto di un pacchetto in un determinato momento della trasmissione al client.

In entrambi gli scenari, il risultato potrebbe essere un errore di scambio EAPoL segnalato e il client verrà deautenticato, dovrà riavviare i processi di associazione e autenticazione.

Per ridurre la probabilità di insorgere di questo problema, utilizzare un timeout più lungo (1000 msec), per concedere più tempo ai client lenti per rispondere. L'impostazione predefinita è 1000 msec, ma potrebbe essere stato impostato manualmente un valore inferiore in modo da consentirne la verifica.

Configurazione

Per configurare questa modifica sono disponibili due meccanismi.

- Globale, disponibile in tutte le release
- Per WLAN, disponibile dalla versione 7.6 alla più recente

L'opzione globale è più semplice e può essere eseguita in tutte le versioni; l'impatto è su tutte le WLAN nel WLC.

L'impostazione di configurazione per WLAN consente un controllo più granulare, con la possibilità di limitare l'impatto dell'SSID, in modo che le modifiche possano essere applicate per tipo di dispositivo, ecc., se raggruppate su wlan specifiche. Disponibile dalla versione 7.6

Ad esempio, potrebbe essere applicata a una WLAN 802.1x generica, ma non a una WLAN specifica della voce, dove potrebbe avere un impatto maggiore

Configurazione globale n. 1:

```
config advanced eap eapol-key-retries 0
```

(opzione solo CLI)

Il valore può essere convalidato con:

```
(2500-1-ipv6) >show advanced eap

EAP-Identity-Request Timeout (seconds)..... 30
```

```
EAP-Identity-Request Max Retries.................. 2

EAP Key-Index for Dynamic WEP..................... 0

EAP Max-Login Ignore Identity Response.......... enable

EAP-Request Timeout (seconds)..................... 30

EAP-Request Max Retries........................... 2

EAPOL-Key Timeout (milliseconds).................. 1000

EAPOL-Key Max Retries............................. 0

EAP-Broadcast Key Interval....................... 3600
```

#2 per configurazione WLAN

X=ID WLAN

```
config wlan security eap-params enable X

config wlan security eap-params eapol-key-retries 0 X
```

Come determinare se un client è stato eliminato a causa di ritrasmissioni senza errori

Il client verrà eliminato perché è stato raggiunto il numero massimo di tentativi EAPoL e verrà deautenticato. Il conteggio di ritrasmissione è 1, come viene contato il fotogramma iniziale

```
 *Dot1x_NW_MsgTask_6: Oct 19 12:44:13.524: 28:34:a2:82:41:f6 Sending EAPOL-Key Message to mobile
28:34:a2:82:41:f6
state PTKINITNEGOTIATING (message 3), replay counter 00.00.00.00.00.00.00.01
..
*osapiBsnTimer: Oct 19 12:44:14.042: 28:34:a2:82:41:f6 802.1x 'timeoutEvt' Timer expired for
station 28:34:a2:82:41:f6 and for message = M3
*Dot1x_NW_MsgTask_6: Oct 19 12:44:14.042: 28:34:a2:82:41:f6 Retransmit failure for EAPOL-Key M3
to mobile 28:34:a2:82:41:f6, retransmit count 1, mscb deauth count 0
..
*Dot1x_NW_MsgTask_6: Oct 19 12:44:14.043: 28:34:a2:82:41:f6 Sent Deauthenticate to mobile on
BSSID 58:ac:78:89:b4:19 slot 1(caller 1x_ptsm.c:602)
```

Rilevamento server non autorizzati

Molte delle tecniche di attacco per le vulnerabilità contro la crittografia PMK/GTK del client, devono "presentare" un falso AP con lo stesso SSID dell'access point dell'infrastruttura, ma che funziona su un canale diverso. Questo può essere facilmente rilevato e l'amministratore di rete può intraprendere azioni fisiche in base ad esso, in quanto si tratta di un'attività visibile.

Sono due i modi proposti finora per fare gli attacchi EAPoL :

- Un falso punto di accesso all'infrastruttura, in altre parole, che agisce da punto di accesso non autorizzato, usando lo stesso indirizzo MAC, di un punto di accesso reale, ma su un canale diverso. Facile da fare per l'aggressore ma visibile

- Inserimento di frame in una connessione valida, forzando il client a reagire. Questo è molto meno visibile, ma rilevabile in alcune condizioni, potrebbe aver bisogno di tempi molto attenti per avere successo

La combinazione delle funzionalità di rappresentazione dell'access point e il rilevamento rogue possono rilevare se un "falso ap" viene inserito nella rete.

Configurazione

- Verificare che il rilevamento rogue sia abilitato sui punti di accesso. Questa opzione è attivata per impostazione predefinita, ma potrebbe essere stata disattivata manualmente dall'amministratore, pertanto deve essere verificata.
- Creare una regola per contrassegnare come dannosi i router che utilizzano "SSID gestiti":
- Verificare che il monitoraggio dei canali sia impostato su "tutti i canali" per entrambe le reti 802.11a/b. L'attacco di base è progettato in modo da essere simile dal punto di vista di RF, il client, su un canale diverso da quello utilizzato sui punti di accesso dell'infrastruttura. Per questo motivo è importante garantire che vengano scansionati tutti i canali possibili:

Rappresentazione AP

Nella configurazione predefinita, l'infrastruttura è in grado di rilevare se lo strumento di attacco utilizza uno dei nostri indirizzi MAC AP. Questo messaggio viene segnalato come trap SNMP e indica che l'attacco sta avendo luogo.

```
Impersonation of AP with Base Radio MAC bc:16:65:13:a0:40 using source address of
bc:16:65:13:a0:40 has been detected by the AP with MAC Address: bc:16:65:13:a0:40 on its
802.11b/g radio whose slot ID is 0
```

Riferimenti

Avviso di sicurezza

Gestione dei problemi in una rete wireless unificata con la versione 7.4 - Cisco

Best practice per la configurazione di Cisco Wireless LAN Controller - Cisco

Rilevamento di anomalie nelle reti wireless unificate - Cisco